METHOD OF SECURE DATA EXCHANGE

Abstract

A method of secure data exchange is applied to a system that includes a server and at least a client. After starting to first connect to the server, the client sends a reset message to the server using an initial key. Once receiving the message, the server verifies the received messages and also uses the initial key to decrypt them. If the verification of the messages is approved, the server generates a first key and sends a key exchange message, which includes the first key and is encrypted by the initial key to the client. Afterward, the client replaces the initial key with the first key in response to the received key exchange message, and meanwhile returns a key confirmation message. If the key confirmation message is approved, the server sends a downloading message to allow the client to retrieve corresponding information. After the information is successfully downloaded, the client sends a finish message to notify the server to await the coming of a next session.